CLAIMS

1. A semiconductor integrated circuit, comprising:

a plurality of selectable pathways inter-connected between a plurality of data sources and data destinations;

a cryptographic circuit connected to the selectable pathways and arranged to selectively receive data at an input from at least one of the data sources, to decrypt or encrypt the data in accordance with a key, and selectively provide the encrypted or decrypted data to at least one of the data destinations via an output;

an instruction interpreter arranged to receive as an input an instruction signal and to generate therefrom an output to control the plurality of selectable pathways to select from which of the data sources the cryptographic circuit receives data and to which destination the cryptographic circuit provides data;

the instruction interpreter configured such that the instruction signal defines a data pathway configuration of the system, and such that it operates in accordance with a rule that limits the data pathway configurations which are selectable.

2. The semiconductor integrated circuit of claim 1 wherein the instruction interpreter is arranged to receive a rule signal defining those data pathway configurations that are unselectable.

3. The semiconductor integrated circuit of claim 2 wherein the rule signal is chosen from a plurality of possible rule signals according to a mode of operation of the system.

4. The semiconductor integrated circuit of claim 3 wherein the rule signal is generated by a rule selector, and wherein the rule selector comprises a plurality of anti-fuses allowing one of a plurality of selectable configurations to be chosen.

5. The semiconductor integrated circuit of claim 4 wherein each of the anti-fuses can be configured once only.

6. The semiconductor integrated circuit of claim 1 wherein the instruction signal is generated by a CPU.

7. The semiconductor integrated circuit of claim 6 wherein the CPU is arranged to generate an instruction signal comprising an instruction portion and a data portion.

8. The semiconductor integrated circuit of claim 1 wherein the instruction signal and rule signal are 32-bit data fields.

9. The semiconductor integrated circuit of claim 1 wherein the plurality of data sources and destinations includes at least one memory for storing encryption or decryption keys.

10. The semiconductor integrated circuit of claim 1 wherein the key is selected from a plurality of keys in dependence on the instruction signal.

11. The semiconductor integrated circuit of claim 10 wherein the key is selected from one of a plurality of key stores and provided to a key input of the cryptographic circuit in dependence on the instruction signal.

12. The semiconductor integrated circuit of claim 10 wherein the cryptographic circuit has a key input, and the key provided to the key input is selected in accordance with the selected pathway.

13. The semiconductor integrated circuit of claim 1 wherein the circuit is arranged to descramble television broadcast signals using a series of control words.

14. The semiconductor integrated circuit of claim 1 wherein the circuit is arranged to decrypt encrypted control words using a service key.

15. The semiconductor integrated circuit of claim 1 wherein the circuit is arranged to decrypt encrypted service keys using a secret key.

16. The semiconductor integrated circuit of claim 1 wherein the circuit is arranged to perform memory-to-memory transfers.

17. The semiconductor integrated circuit of claim 12 wherein the plurality of selectable pathways are configurable such that when the data from the data source is a service key, the cryptographic circuit receives a secret key at the key input.

18. The semiconductor integrated circuit of claim 12 wherein the plurality of selectable pathways are configurable such that when the data source is a memory and the data destination is a memory, the cryptographic circuit (9) receives a software written key at the key input.

19. The semiconductor integrated circuit of claim 12 wherein the plurality of selectable pathways are configurable such that when the data source is a plurality of control words, the cryptographic circuit receives a service key at the key input.

20. The semiconductor integrated circuit of claim 12 wherein the plurality of selectable pathways are configurable such that when the data source is

broadcast data, the cryptographic circuit receives a software written key at the key input.

21. The semiconductor integrated circuit of claim 9 wherein one of the key memories stores at least one key generated by a software algorithm.

22. The semiconductor integrated circuit of claim 9 wherein one of the key memories stores at least one service key for decrypting control words.

23. The semiconductor integrated circuit of claim 9 wherein one of the key memories stores a secret key for decrypting service keys.

24. The semiconductor integrated circuit of claim 1 wherein the plurality of data sources and destinations includes at least one of a hard disc, ROM, RAM, data in port and data out port.

25. The semiconductor integrated circuit of claim 1 wherein the cryptographic circuit is an AES circuit.

26. The semiconductor integrated circuit of claim 1 wherein the plurality of selectable pathways are selected by at least one multiplexor or switch.

27. The semiconductor integrated circuit of claim 1 wherein the instruction interpreter comprises a plurality of combinatorial components arranged such that the output is generated as a function of the instruction signal.

28. The semiconductor integrated circuit of claim 1 wherein the encryption system is a subscriber-based pay-television system.

29. The semiconductor integrated circuit of claim 1 wherein the encryption system is a monolithic integrated circuit.

30. A method of configuring a circuit for selecting routing rules in an encryption system, comprising: configuring one or more of a plurality of anti-fuses within the circuit such that the circuit is configured to select routing rules according to a rule selection scheme, wherein the rule selection scheme depends upon the configuration of the circuit and wherein each of the anti-fuses can be configured once only.

31. An encryption and decryption method, comprising:

generating an instruction signal containing an instruction portion and a data portion;

receiving data at a cryptographic circuit from one of the plurality of data sources on a data pathway selected in response to the instruction signal;

performing one of encryption and decryption on the data in response to the instruction signal; and

thereafter providing the encrypted/decrypted data to one of a plurality of data destinations on a data pathway selected in response to the instruction signal.

32. An encryption/decryption method, comprising:

configuring one or more of a plurality of anti-fuses within a rule selector circuit such that the rule selector circuit is configured to select a routing rule according to a rule selection scheme, the rule selection scheme depending upon the configuration of the encryption/decryption circuits;

generating an instruction signal in accordance with the routing rule received from the rule selection circuit;

receiving data at a cryptographic circuit from one of a plurality of data sources on a data pathway selected in response to the instruction signal;

performing one of encryption and decryption on the data in response to the instruction signal; and

thereafter providing the encrypted/decrypted data to one of a plurality of data destinations on a data pathway selected in response to the instruction signal.

33. The method of claim 32 wherein configuring one or more of a plurality of anti-fuses comprises configuring one or more of the plurality of anti-fuses only once.

34. The method of claim 32, comprising receiving encrypted control words and a service key and decrypting the service key with a secret key to decrypt the encrypted control words.

35. A method of encrypting and decrypting data in an encryption/decryption circuit, the method comprising:

storing a plurality of encryption and decryption keys;

configuring one or more of a plurality of one-time switches in a rule selection circuit to select one from among a plurality of routing rules according to a rule selection scheme dependent upon a configuration of the encryption/decryption circuit;

generating an instruction signal containing an instruction portion and a data portion, the instruction signal configured to select an encryption/decryption key;

receiving data at a cryptographic circuit from one of a plurality of data sources on a data pathway selected in response to the instruction signal, including receiving encrypted control words and a service key;

performing one of decryption and encryption on the data in response to the instruction signal, including decrypting the service key with a secret key stored in the encryption/decryption circuit in order to decrypt the encrypted control words; and

thereafter providing the encrypted/decrypted data to one of a plurality of data destinations on a data pathway selected in response to the instruction signal.

36. A decryption/encryption circuit for use in a semiconductor integrated circuit, comprising:

a plurality of data sources and data destinations coupled via a plurality of data pathways;

a rule selection circuit having one-time selectable switches for selecting one from among a plurality of routing rules in accordance with a rule selection scheme;

a central processing unit configured to generate an instruction signal for selecting and unselecting data pathways in accordance with a routing rule generated by the rule selection circuit, the instruction signal including instructions for selecting a key from a key store;

an instruction interpreter coupled to the rule selection circuit and the central processing unit and configured to receive the routing rule and the instruction signal and generate an output signal; and

a cryptographic circuit coupled to the instruction interpreter and selectively coupleable to one or more of the data pathways in response to the output of the instruction interpreter to receive data at an input from at least one of the data sources on a data pathway in response to the instruction signal, to decrypt or encrypt the data in accordance with a key selected in response to the instruction signal, and to thereafter provide encrypted/decrypted data to one of the plurality of data destinations on a data pathway selected in response to the instruction signal.

37. The circuit of claim 36 wherein the data received at the cryptographic circuit includes encrypted control words and a service key, and wherein the cryptographic circuit is configured to utilize the key from the instruction signal to decrypt the service key and thereafter decrypt the encrypted control words in accordance with the decrypted service key.